

Exercise 3 – Chinese Remainder theorem, rings

October 14, 2026

Problem 1. Find all $x \in \mathbb{Z}$ satisfying:

- a) $x \equiv 1 \pmod{3}$, $x \equiv 3 \pmod{5}$,
- b) $x \equiv 2 \pmod{3}$, $x \equiv 4 \pmod{7}$, $x \equiv 3 \pmod{8}$,
- c) $10x \equiv 6 \pmod{32}$, $3x \equiv 1 \pmod{5}$.

Problem 2. Find an example that illustrates the necessity of the pairwise coprimality assumption on the integers m_i in the Chinese Remainder Theorem.

Problem 3. $\triangleleft$ The Chinese commander Zhuge Liang commanded a unit of 1,000 men. However, many of his men fell in the Battle of Chibi. To avoid having to count them one by one, he ordered them to form rows of 7, leaving 2 men left over. He then ordered them to form rows of 11, leaving 6 men left over. Finally, he arranged them in rows of 13, leaving just one man left over. The commander now knew how many men had survived. How many were there?

Note: Zhuge Liang really did live and fight in the Battle of Chibi. He was a strategist, inventor, philosopher, provincial administrator, and probably a good mathematician as well. However, he probably did not know the Chinese Remainder Theorem.

Problem 4. $\triangleleft$ Use the Chinese Remainder Theorem to compute $12^{100} \pmod{30}$.

Hint: Use $\pmod{5}$ and $\pmod{6}$.

Problem 5. Determine whether each of the following structures is a field, an integral domain, or a ring:

- a) $\mathbb{Z}_n$, where $n \in \mathbb{N}$, with the usual addition and multiplication,
- b) $\mathbb{Z} \times \mathbb{Z}$, with addition and multiplication defined componentwise,
- c) the 2×2 matrices over the field $\mathbb{Z}_7$, denoted by $M_2(\mathbb{Z}_7)$, with matrix addition and multiplication,
- d) the upper triangular 3×3 matrices over $\mathbb{Q}$, with matrix addition and multiplication,
- e) $\mathbb{Z}[i]$, the complex numbers with integer coefficients, with the usual addition and multiplication,
- f) $\mathbb{Q}[i]$, the complex numbers with rational coefficients, with the usual addition and multiplication,
- g) $\mathbb{Z}[[x]]$, the set of all formal power series with integer coefficients, with the usual addition and multiplication,
- h) $\mathbb{H}$, the quaternions, consisting of real numbers extended by the imaginary units i, j, k , satisfying $i^2 = j^2 = k^2 = ijk = -1$,
- i) for an arbitrary set S , define a structure on $\mathcal{P}(S)$ in which addition of two sets is their symmetric difference and multiplication is their intersection,
- j) $\mathbb{Z}$, where addition is defined as the maximum of two integers and multiplication as the greatest common divisor of two integers.

Problem 6. Let $\mathbb{C}$ be the field of complex numbers. Consider the following subsets:

- a) $R_1 = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$,
- b) $R_2 = \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Z}\}$,
- c) $R_3 = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$,
- d) $R_4 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

Determine which of the sets R_i are subrings of $\mathbb{C}$ and which are subfields of $\mathbb{C}$.

Homework. Prove that commutativity of addition follows from the other axioms of a commutative ring.